#2

PATENT
3667-0102P

1-11-02

IN THE U.S. PATENT AND TRADEMARK OFFICE

Applicant:	QIN, Simon	Conf.:	
Appl. No.:	09/750,160	Group:	2825
Filed:	December 29, 2000	Examiner:	UNASSIGNED

For: BACKUP/RECOVERY SYSTEM AND METHODS FOR PROTECTING A COMPUTER SYSTEM

L E T T E R

Assistant Commissioner for Patents
Washington, DC 20231

June 21, 2001

Sir:

Under the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55(a), the applicant(s) hereby claim(s) the right of priority based on the following application(s):

Country	Application No.	Filed
TAIWAN, R.O.C.	089126682	December 14, 2000

A certified copy of the above-noted application(s) is(are) attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fee required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By Joe McKinney Muncy
Joe McKinney Muncy, #32,334

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000

KM/asc
3667-0102P

Attachment

(Rev. 01/22/01)

Attorney Docket No. 3667-0102P
December 29 2000
QIN, SIMON
Birch, Stewart, Kolasch & Birch, LLP
(703) 205-8000

OIPE JC184 JUN 21 2001 PATENT & TRADEMARK OFFICE

中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下 ：

This is to certify that annexed is a true copy from the records of thi
office of the application as originally filed which is identified here

申　請　日 ： 西元 2000 年 12 月 14 日
Application Date

申 請 案 號 ： 089126682
Application No.

申　請　人 ： 東石資訊股份有限公司
Applicant(s)

RECEIVED
DEC 26 2001
Technology Center 2100

CERTIFIED COPY OF
PRIORITY DOCUMENT

局　　長
Director General

陳明邦

發文日期： 西元 2001 年 3 月 日
Issue Date

發文字號： 09011003747
Serial No.

RECEIVED
JUL 25 2001
TC 2800 MAIL ROOM

申請日期：	案號：
類別：	

（以上各欄由本局填註）

發明專利說明書

一、發明名稱	中文	備份/還原系統及其方法
	英文	Backup/recovery system and method for protecting a computer system
二、發明人	姓名（中文）	1.覃云川
	姓名（英文）	1.Simon Qin
	國籍	1.中國
	住、居所	1.重慶市沙坪壩區沙坪壩北街83號
三、申請人	姓名（名稱）（中文）	1.東石資訊股份有限公司
	姓名（名稱）（英文）	1.Far Stone Technology Inc.
	國籍	1.中華民國
	住、居所（事務所）	1.台北市內湖區洲子街101號6樓
	代表人姓名（中文）	1.林北湖
	代表人姓名（英文）	1.Pei hu Lin

四、中文發明(發明之名稱：備份/還原系統及其方法)

一種備份/還原系統及其方法，可藉以即時進行備份/還原的動作，其可適用於一電腦系統，上述電腦系統至少具有一應用層，上述應用層耦接於一介面，於上述應用層執行既定之應用程式，其特徵在於：上述備份/還原系統安裝於上述電腦系統，上述備份/還原系統包括一監測模組，上述監測模組加入上述電腦系統進行監測，當於接收一既定資料時，上述監測模組監測上述既定資料，並判知其中是否具有既定的危害性資料，以判斷上述備份/還原系統是否進行資料備份，再經該介面進行一既定處理後，通知上述應用層進行擷取；藉此，上述備份/還原系統可達成有效監測，全面防護電腦系統硬碟毀損。

英文發明摘(發明之名稱：Backup/recovery system and method for protecting a computer system)

本 案 已向

國（地區）申請專利　　申請日期　　案號　　主張優

無

有關微生物已寄存於　　寄存日期　　寄存號碼

無

五、發明(說)明

本發明是有關於電腦系統之備份/還原技術，且特別是有關於一種可還原硬碟到正常狀態之系統及其方法，其可以在接收網路資料之前即時建立還原點，將有效資料的資訊記入還原點，以在意外發生的情況下，將電腦系統還原到該行為之前硬碟的狀態。

電腦系統的防護是目前電腦使用者之重要議題。由於網路蓬勃發展，藉由Internet來散播病毒訊息的連鎖信也愈來愈多，現代人在習慣了電子郵件作為人與人之間溝通的介面之後，經常性地會收到來自各方關心問候與訊息傳遞，當然，也難免地會收到惱人的廣告信函（或稱垃圾信）以及令人防不甚防的夾帶病毒。

在近日，病毒常以email夾帶附加檔案「.EXE」（或.DOC）來進行散播。當使用者在不知情的狀況下執行該附帶檔，電腦隨即中毒。病毒會將自己寄給使用者通訊錄裡所有的名單，若使用者不對其存有戒心並執行病毒檔案，在執行附加檔後將造成連鎖性的感染，致在世界各地傳出感染災情。

對個人電腦使用者來說，上網之時常面對諸多危險，若不慎感染到病毒，病毒常會破壞使用者硬碟的檔案，可能會刪除所有磁碟中的全部檔案，致重要資料瞬間遭刪除，且造成電腦無法正常運作。若作業系統檔案遭感染破壞，將造成Windows無法重新開機，系統需要重灌等嚴重後果。因而日常之中，防毒之心理不可無，防毒的措施亦不可少。

五、發明(說)明

習用的備份/還原軟體，縱然有備份/還原的功能，可以執行備份程式來備份資料，亦或是執行還原程式將資料還原到硬碟，以保護硬碟回到正常狀態，但無論是工作端硬碟未受到完全的保護，亦或是備份/還原動作所耗費的時間極為冗長，無法滿足使用者即時備份/還原的需求，都會造成使用者頭疼問題。

例如，美國Symantec Inc.公司之Ghost備份/還原軟體，其備份/還原動作需要在執行備份/還原程式之前先執行作業系統，並且需由網路管理者以手動方式執行備份/還原。Ghost備份可以將選定的硬碟/硬碟分區完全備份到檔案，Ghost還原可以將資料從檔案還原到選定的硬碟/硬碟分區，建立備份是一個單任務過程，需要先停止其他任務，佔用一段約長達8分鐘/Gb的時間。使用Ghost軟體備份資料所佔用的磁碟空間相當大，因為 Ghost軟體所備份的資料是硬碟上所有的有效資料，只要是在作業系統的檔案系統裏有被使用的資料，即完全對此區域的資料作備份到檔案，而不論其後來是否被改變。

再有美國Roxio, Inc.公司之Goback備份/還原軟體，其執行還原程式之前不需要先執行作業系統，指示系統開始還原作業之後，Goback即將硬碟還原到選定的狀態。在系統遭到破壞之時，還原硬碟的動作也需由網路管理者以手動方式執行還原程式將資料還原。

顯然地，電腦系統於上網或接收電子郵件之時，常因下載行為不慎感染到病毒，病毒發作致系統毀損等意外時

時發生，甚至無法開機。但，在習知技藝中，備份/還原軟體並無法有效地識別由網路接收資料所可能帶來的危害性，更加無法即時將資料進行備份。

而，習用的防毒軟體，如趨勢科技的網際網路病毒防火牆，提供網路入門閘道的防護功能，防止電腦病毒以及惡性程式的入侵。在閘道口偵測攔截Internet從SMTP、HTTP、以及 FTP 管道進入的病毒，並將惡性程式在閘道口攔截下來。於偵測到病毒或入侵活動時，可以採取警示系統管理人員的措施，且刪除中毒檔案或在管制條件下允許使用者下載中毒檔案或隔離該檔案後續再處理。

雖然，習用的防毒軟體可以在上網時提供Internet即時防毒服務，攔截Internet電子郵件病毒，但是未具有備份/還原的技術，完全無法備份資料，系統毀損時亦無法將資料還原到硬碟，使硬碟回到正常狀態，不能滿足使用者即時備份/還原的需求。

有鑑於目前防毒軟體無備份/還原的功能，且沒有任何其他備份/還原軟體產品可以識別網路接收資料可能的危害性而採取電腦系統的保護措施，本發明便提供一種保護電腦系統的備份/還原系統及其方法，其具有全面防護電腦系統硬碟毀損的機制，即便是網路資料夾帶有病毒，亦可確保電腦系統不受到破壞。

本發明之備份/還原系統可安裝於上述電腦系統，用以即時監測及備份資料，上述電腦系統至少具有一應用層耦接於一介面，上述備份/還原系統包括一監測模組，上

述監測模組加入上述電腦系統進行監測。

根據上述，當於接收一既定資料時，上述監測模組監測上述既定資料，並判知其中是否具有既定的危害性資料，以判斷上述備份/還原系統是否建立一還原點，再經該介面進行一既定處理後，通知上述應用層進行擷取。

本發明之備份/還原系統的處理方法，上述備份/還原系統可適用於一電腦系統中，上述處理方法包括下列步驟：上述備份/還原系統監測是否有來自網路的既定資訊；當上述備份/還原系統接收到上述既定資訊時，判知其中是否具有既定的危害性資料；以及當上述既定資訊中具有上述既定的危害性資料時，上述備份/還原系統建立一還原點。

本發明另提供一種藉備份/還原系統保護電腦系統之方法，上述電腦系統包括一應用層，上述應用層耦接於一介面，於上述應用層執行既定之應用程式，其包括下列步驟：安裝上述備份/還原系統於上述電腦系統，上述備份/還原系統包含的一監測模組加入上述電腦系統進行監測；上述監測模組於上述驅動層監測來自網際網路的既定資訊，判知其中是否具有既定的危害性資料；當上述既定資訊中具有上述既定的危害性資料時，上述備份/還原系統建立一還原點；以及經該介面進行一既定處理後，通知上述應用層進行擷取。

其中，上述備份/還原系統可安裝於複數用戶端所建構而得之一網路。上述網路係經由一伺服器端進行管理，

五、發明(說)明

上述伺服器端可以遠端即時控制上述用戶端的備份/還原行為。上述網路所使用之傳輸協定為TCP/IP。

其中，上述既定資料係來自網際網路(Internet)的下載行為或以 Outlook Express 接收電子郵件的資料。上述既定的危害性資料係有危害性的資料或可能有危害性的資料，包括EXE資料或DOC資料。

為讓本發明之上述和其他目的、特徵、和優點能更明顯易懂，下文特舉一較佳實施例，並配合所附圖式，作詳細說明如下：

較佳實施例

本發明之備份/還原系統係採用即時的備份/還原技術，以監測網路行為的機制，全面防護電腦系統硬碟毀損。在本較佳實施例中，藉由監測的功能，可在網路資料接收之前即時建立還原點，以將有效資料的資訊記入還原點。不過，對於熟習此技術者而言，本發明亦可經調整而應用於其他需要監測網路行為之應用。

本發明較佳實施例之備份/還原系統，安裝於一電腦系統，上述電腦系統至少具有一應用層耦接於一介面，於上述應用層執行既定之應用程式。上述備份/還原系統包括一監測模組，上述監測模組加入上述電腦系統進行監測。

當於接收一既定資料時，上述監測模組監測上述既定

資料，並判知其中是否具有既定的危害性資料，以判斷上述備份/還原系統是否建立一還原點進行資料備份，再經該介面進行一既定處理後，通知上述應用層進行擷取。

第1圖係本發明較佳實施例之安裝於電腦系統的部分結構示意圖。於本較佳實施例中，備份/還原軟體可有效地識別由網路接收資料所可能帶來的危害性，可即時建立還原點將資料進行備份。

電腦系統可包括有一應用層（Application Layer）2及一驅動層（Driver Layer）4，於應用層2執行既定之應用程式，而於驅動層4執行既定之驅動程式。應用層2耦接於一網路介面，該網路介面係在初始化時將相應的協定模組安裝內儲。

應用層2是Windows應用程式執行的層面，使用者通過此介面程式實施各種功能，例如還原等。所有網路應用程式，包括Internet Explorer, Outlook Express, FTP utilities, TELNET utilities等，都運行在應用層2，其具有一網際網路應用介面（Internet Application）20。

驅動層4是Windows驅動程式執行的層面，所有網路驅動程式都執行在驅動層4，其向應用程式提供網路存取服務，向下則通過網路介面卡或其他網路設備存取LAN(局部區域網路）及Internet(網際網路）6，其具有一網路驅動介面（Network driver）40。

備份/還原系統係可安裝於複數用戶端所建構而得之

一網路，該等用戶端間可以通訊協定進行傳輸，例如，TCP/IP（傳輸控制/網路通訊協定）。網路可由一伺服器端進行管理，伺服器端可以遠端即時控制用戶端的備份/還原行為。

備份/還原系統包括有一監測模組42，一個網路監測驅動介面（network monitor driver），安裝於電腦系統以後，監測模組42可加入應用層2或驅動層4，而於本較佳實施例中，備份/還原系統係向驅動層4中加入監測模組42來進行監測，實行對網路資料的攔截。

當電腦系統接收一既定資料時，監測模組42監測上述既定資料。上述既定資料係來自網際網路(Internet)的下載行為或以 Outlook Express 接收電子郵件的資料，包括HTTP pages、E-mails、downloading files等等。

並且，監測模組42判知其中是否具有既定的危害性資料，以判斷備份/還原系統是否建立一還原點進行資料備份。上述既定的危害性資料係有危害性的資料或可能有危害性的資料，其包括有.EXE檔資料，.DOC檔資料，.ZIP檔資料，或其他可能對系統具有危險性的其他類型檔。

也就是說，應用層2所有訪問Internet而下載資料或打開Outlook Express收取郵件時，監測模組42會識別到電腦系統要接收資料加以監測，如果發現下載資料或郵件中有病毒或都是其他任何的有危害的文件時，則在該資料到達電腦系統之前，備份/還原系統會自動建立一個還原點備份資料。

其後，監測模組42會把既定資料返回，經該網路介面進行一既定處理，例如，進行協定模組相應處理，及對所接收之數據進行統一的格式處理，在此之後，再通知應用層2進行上述既定資料擷取。

至此，接收既定資料後如果既定資料對電腦系統硬碟有任何的破壞，那麼在意外發生的情況下，可將電腦系統硬碟上的資料恢復到網路行為接收既定資料之前硬碟的狀態。

根據上述，本較佳實施例之備份/還原系統可在電腦系統上偵測來自Internet的所有資訊，一旦識別出以上下載行為或打開Outlook Express收取郵件，就立即建立一個新的還原點，將有效資料的資訊記入還原點。

監測模組42全程監視所有來自Internet的資料，因此，如果接收之資料、新下載的檔案包含著病毒或其他惡意程式，即使它發作而導致系統毀損，也可以將硬碟還原到之前的狀態。

本發明較佳實施例之備份/還原系統的處理方法中，上述備份/還原系統可適用於一電腦系統，上述處理方法包括下列步驟：上述備份/還原系統監測是否有來自網路的既定資訊；當接收到上述既定資訊時，判知其中是否具有既定的危害性資料；以及當具有上述既定的危害性資料時，上述備份/還原系統建立一還原點進行資料備份。

本較佳實施例中，藉備份/還原系統保護電腦系統，上述電腦系統包括一應用層，上述應用層耦接於一介面，

於上述應用層執行既定之應用程式，其保護方法包括下列步驟：安裝上述備份/還原系統於上述電腦系統，上述備份/還原系統包含的一監測模組加入上述電腦系統進行監測；上述監測模組於上述驅動層監測來自網際網路的既定資訊，判知其中是否具有既定的危害性資料；當上述既定資訊中具有上述既定的危害性資料時，上述備份/還原系統建立一還原點進行資料備份；以及經該介面進行一既定處理後，通知上述應用層進行擷取。

請參考第2圖，其係本發明較佳實施例之安裝於電腦系統的工作流程圖。首先，於步驟S10，當有網路資料到達時，監測模組42先於應用程式接收到這些網路資料，接收到以後進行監測。

接著於步驟S30，監測模組42監測網路資料是否是下載行為，並分析這些資料所含內容，判斷是否使用者請求的既定資料。如果不是，則直接到步驟S90，並將網路資料傳遞給上層應用程式。

如果是，則接著到步驟S50。上述既定資料係來自網際網路(Internet)的下載行為或以 Outlook Express 接收電子郵件的資料，包括HTTP pages、E-mails、downloading files等等。

於步驟S50，監測模組42進一步判斷上述既定資料是否含有可能具有危害性的資料(例如可能帶有病毒的EXE, DOC, Mail等)。如果不是(例如TXT,bitmap等資料)，則亦直接到步驟S90，監測模組42把既定資料傳遞

給上層應用程式。

如果是，則接著到步驟S70。因為監測模組42發現下載資料或郵件中有病毒或都是其他任何的有危害的文件時，所以在該資料到達電腦系統之前，備份/還原系統自動建立一個還原點。

最後，於步驟S90，監測模組42再將資料傳遞，經該網路介面進行一既定處理，如協定模組相應處理及對所接收之數據統一的格式處理，在此之後，再通知應用層2進行上述既定資料擷取。

因此，如果接收既定資料後，既定資料對電腦系統硬碟有任何的破壞，那麼在發生意外的情況下，電腦系統硬碟上的資料可恢復到接收資料之前硬碟的狀態。

其中，步驟S70建立一個還原點的流程，係先掃描整個硬碟，辨認有效資料。每一個還原點裏都包含著硬碟上哪些資料是有效資料的資訊，建立新還原點的時候，將有效資料的資訊記入還原點。

值得注意的是，MSTCP協定（Microsoft定義之TCP協定）與Http/Ftp/POP3等高層協定的通信是通過TDI(Transport Driver Interface；傳輸驅動介面)層來實現，而本發明較佳實施例之監測模組42係於TDI層對網路資料進行監測攔截。

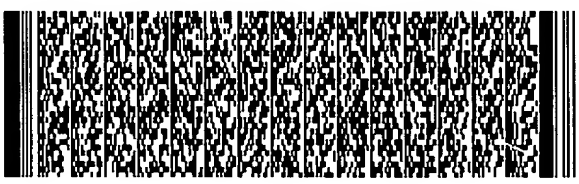
高層通信協定通過TDI層的入口函數TdiSendEntry()來向Internet發送資料，而Internet返回資料時，MSTCP協定產生一個TDI_EVENT_RECEIV的事件，調用由

SetEventEntry()所設置的事件處理函數還處理這個事件。由於應用層所有訪問Internet的函數介面都是通過入口位址全局表實現的，因此，在TDI層的驅動程式更改表中的函數入口位址，更改TdiSendEntry()和SetEventEntry()函數的入口，就可以實行對Internet資料的攔截。

當有不安全文件文件下載時，如下列情況即可通知備份/還原系統自動建立還原點。當打開Outlook Express收取郵件時，Outlook Express會向Internet上的郵件伺服器發送收取郵件的請求，此時Outlook Express向Internet發送的所有的資料都會通過TDI層來，而TDI層的驅動程式會識別到用戶要收取郵件，驅動程式修改從Internet上的郵件伺服器返回郵件的事件的入口位址。當有郵件返回時，系統就會首先調用驅動程式的事件處理函數，事件處理函數處理郵件包含的資料，如果發現郵件中有病毒或是其他任何的有危害的文件時，驅動程式會通知備份/還原系統的驅動程式建立一個新的還原點。

新的還原點在備份資料的過程中，根據此類資料判定哪些資料是需要備份的，哪些資料是不需要備份的。本發明較佳實施例將有效資料資訊記入還原點，完成建立還原點。

之後，驅動程式會把郵件返回給Outlook Express。至此，使用者打開郵件後，如果郵件對硬碟有任何的破壞，那麼使用者就可以把硬碟上的資料恢復到收郵件前的

狀態。

請參考第3圖，其係顯示於本發明實施例中，將電腦系統硬碟還原到之前的狀態。如圖所示，電腦系統硬碟狀態A是在健康的狀態，此時由於監測模組42判知上述既定資料中具有既定的危害性資料，因此，備份/還原系統自動建立一個還原點。

接著，監測模組42會把既定資料返回，資料到達電腦系統，經該網路介面進行一既定處理之後，應用層2擷取上述既定資料，下載一個帶有病毒的程式UNKNOWN.EXE，但使用者並不知情。

既定資料帶有病毒，電腦系統硬碟狀態B是在帶有病毒的狀態。之後，病毒被執行，並對電腦系統硬碟進行破壞，硬碟狀態C是在被破壞的狀態。但是，在意外發生的情況下，使用者可藉本較佳實施例之備份/還原系統將硬碟上的資料恢復到網路行為接收既定資料之前硬碟的狀態。

所以，雖然電腦系統於上網或接收電子郵件之時，因下載行為不慎感染到病毒，致病毒發作毀損系統，但，本發明較佳實施例備份硬碟上發生改變的有用資料，可以使硬碟自動還原到正常的狀態，系統及應用程式永遠不會受到毀損或丟失。

雖然本發明以前述之較佳實施例揭露如上，然其並非用以限定本發明，任何熟習此技藝者，在不脫離本發明之精神和範圍內，當可作些許之更動與潤飾，因此本發明之

五 、發明(說)明

保護範圍當視後附之申請專利範圍所界定者為準。

圖式簡單說明

第1圖係本發明較佳實施例之安裝於電腦系統的部分結構示意圖；

第2圖係本發明較佳實施例之安裝於電腦系統的工作流程圖；

第3圖係顯示於本發明實施例中，將電腦系統硬碟還原到之前的狀態。

六、申請專利範圍

1.一種備份/還原系統，其可適用於一電腦系統，上述電腦系統至少具有一應用層，上述應用層耦接於一介面，於上述應用層執行既定之應用程式，其特徵在於：

上述備份/還原系統安裝於上述電腦系統，上述備份/還原系統包括一監測模組，上述監測模組加入上述電腦系統進行監測，當於接收一既定資料時，上述監測模組監測上述既定資料，並判知其中是否具有既定的危害性資料，以判斷上述備份/還原系統是否進行資料備份，再經該介面進行一既定處理後，通知上述應用層進行擷取。

2.如申請專利範圍第1項所述之備份/還原系統，其可安裝於複數用戶端所建構而得之一網路。

3.如申請專利範圍第2項所述之備份/還原系統，其中，上述網路係經由一伺服器端進行管理。

4.如申請專利範圍第3項所述之備份/還原系統，其中，上述伺服器端可以遠端即時控制上述用戶端的備份/還原行為。

5.如申請專利範圍第3項所述之備份/還原系統，其中，上述網路所使用之傳輸協定為TCP/IP。

6.如申請專利範圍第1項所述之備份/還原系統，其中，上述既定資料係來自網際網路(Internet)的下載行為。

7.如申請專利範圍第1項所述之備份/還原系統，其中，上述既定資料係以 Outlook Express 接收電子郵件。

8.如申請專利範圍第1項所述之備份/還原系統，其中，上述既定的危害性資料係有危害性的資料。

六、申請專利範圍

9.如申請專利範圍第1項所述之備份/還原系統，其中，上述既定的危害性資料係可能有危害性的資料。

10.如申請專利範圍第1項所述之備份/還原系統，其中，上述既定的危害性資料包括EXE資料。

11.如申請專利範圍第1項所述之備份/還原系統，其中，上述既定的危害性資料包括DOC資料。

12.一種備份/還原系統的處理方法，上述備份/還原系統可適用於一電腦系統中，上述處理方法包括下列步驟：

上述備份/還原系統監測是否接收一既定資料；

當上述備份/還原系統接收到上述既定資料時，判知其中是否具有既定的危害性資料；以及

當上述既定資訊中具有上述既定的危害性資料時，上述備份/還原系統進行資料備份。

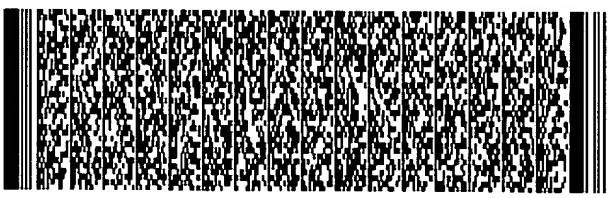
13.如申請專利範圍第12項所述之備份/還原系統的處理方法，其中，上述備份/還原系統安裝於由複數用戶端所建構而得之一網路。

14.如申請專利範圍第13項所述之備份/還原系統的處理方法，其中，上述網路係經由一伺服器端進行管理。

15.如申請專利範圍第14項所述之備份/還原系統的處理方法，其中，上述伺服器端可以遠端即時控制上述用戶端的備份/還原行為。

16.如申請專利範圍第14項所述之備份/還原系統的處理方法，其中，上述網路所使用之傳輸協定為TCP/IP。

17.如申請專利範圍第12項所述之備份/還原系統的處理方



六、申請專利範圍

法，其中，上述既定資料係來自網際網路(Internet)的下載行為。

18.如申請專利範圍第12項所述之備份/還原系統的處理方法，其中，上述既定資料係以 Outlook Express 接收電子郵件。

19.如申請專利範圍第12項所述之備份/還原系統的處理方法，其中，上述既定的危害性資料係有危害性的資料。

20.如申請專利範圍第12項所述之備份/還原系統的處理方法，其中，上述既定的危害性資料係可能有危害性的資料。

21.如申請專利範圍第12項所述之備份/還原系統的處理方法，其中，上述既定的危害性資料包括EXE資料。

22.如申請專利範圍第12項所述之備份/還原系統的處理方法，其中，上述既定的危害性資料包括DOC資料。

23.一種藉備份/還原系統保護電腦系統之方法，上述電腦系統包括一應用層，上述應用層耦接於一介面，於上述應用層執行既定之應用程式，其包括下列步驟：

安裝上述備份/還原系統於上述電腦系統，上述備份/還原系統包含的一監測模組加入上述電腦系統進行監測；

上述監測模組監測一既定資料，判知其中是否具有既定的危害性資料；

當上述既定資訊中具有上述既定的危害性資料時，上述備份/還原系統進行資料備份；以及

經該介面進行一既定處理後，通知上述應用層進行擷取。

六、申請專利範圍

24.如申請專利範圍第23項所述之方法，其中，上述備份/還原系統安裝於複數用戶端所建構而得之一網路。

25.如申請專利範圍第24項所述之方法，其中，上述網路係經由一伺服器端進行管理。

26.如申請專利範圍第25項所述之方法，其中，上述伺服器端可以遠端即時控制上述用戶端的備份/還原行為。

27.如申請專利範圍第25項所述之方法，其中，上述網路所使用之傳輸協定為TCP/IP。

28.如申請專利範圍第23項所述之方法，其中，上述既定資料係來自網際網路(Internet)的下載行為。

29.如申請專利範圍第23項所述之方法，其中，上述既定資料係以 Outlook Express 接收電子郵件。

30.如申請專利範圍第23項所述之方法，其中，上述既定的危害性資料係有危害性的資料。

31.如申請專利範圍第23項所述之方法，其中，上述既定的危害性資料係可能有危害性的資料。

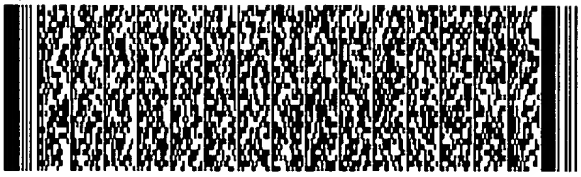
32.如申請專利範圍第23項所述之還原系統的處理方法，其中，上述既定的危害性資料包括EXE資料。

33.如申請專利範圍第23項所述之還原系統的處理方法，其中，上述既定的危害性資料包括DOC資料。

申 請 案 件 名 稱 :備 份 /還 原 系 統 及 其 方 法

第 1/21 頁

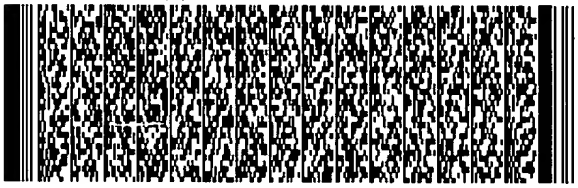
第 2/21 頁



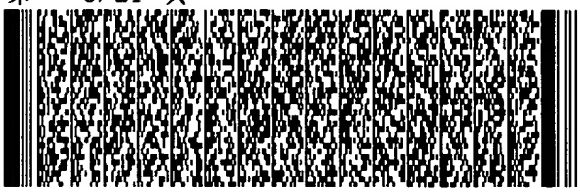
第 4/21 頁

第 4/21 頁

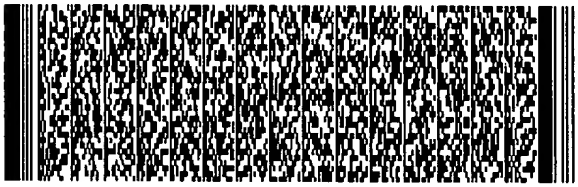
第 5/21 頁



第 5/21 頁

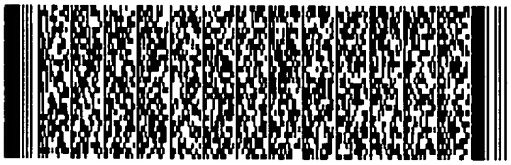


第 6/21 頁

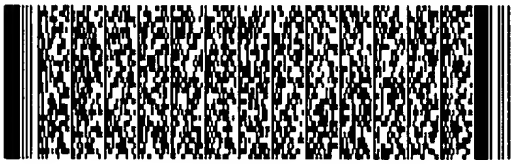


第 6/21 頁

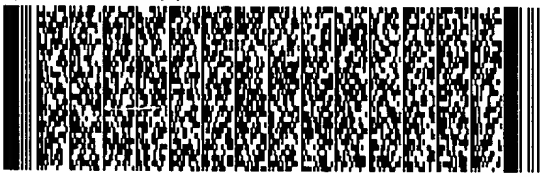
第 7/21 頁



第 7/21 頁

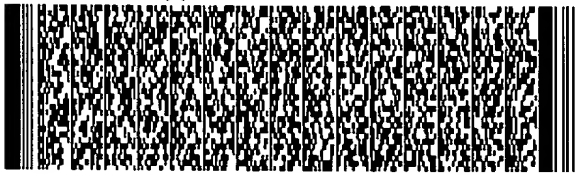


第 8/21 頁

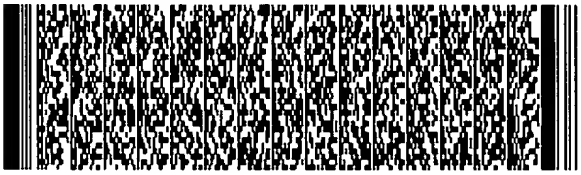


第 8/21 頁

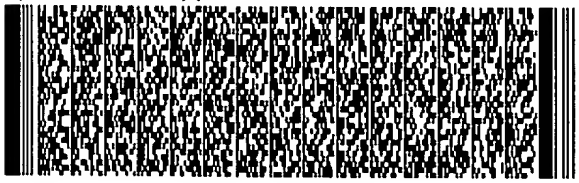
第 9/21 頁



第 9/21 頁

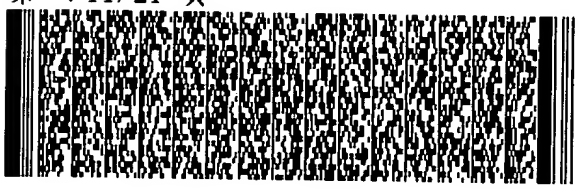


第 10/21 頁

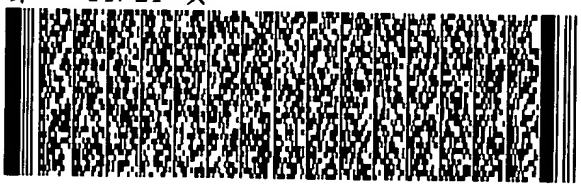


第 10/21 頁

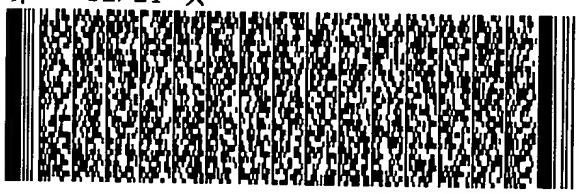
第 .11/21 頁



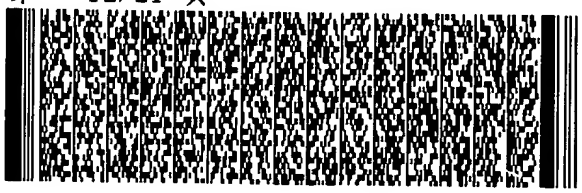
第 11/21 頁



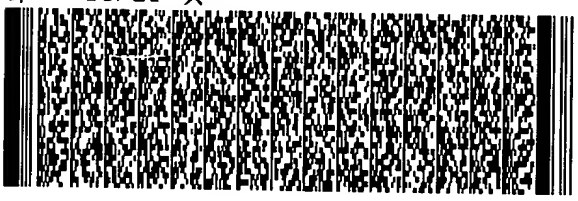
第 12/21 頁



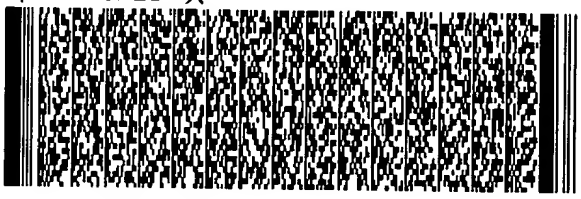
第 12/21 頁



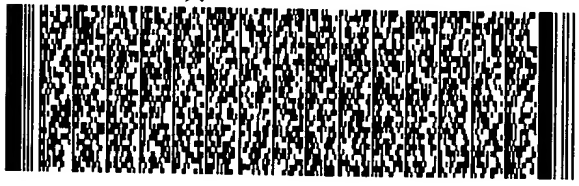
第 13/21 頁



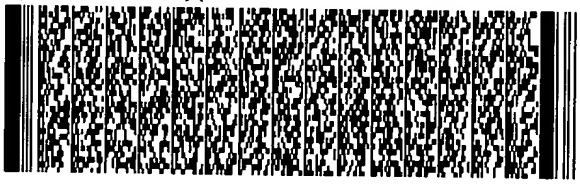
第 13/21 頁



第 14/21 頁

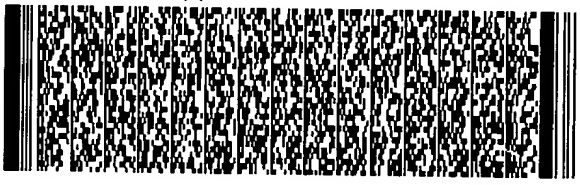


第 14/21 頁



第 15/21 頁

第 15/21 頁

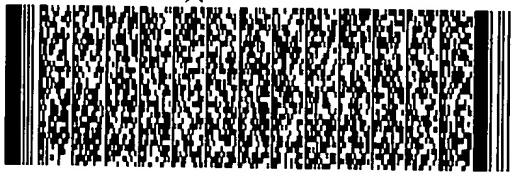


第 16/21 頁

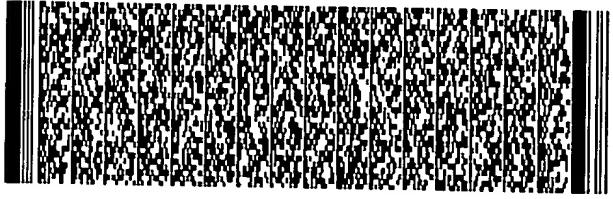
第 17/21 頁

第 18/21 頁

第 18/21 頁



第 19/21 頁



第 20/21 頁

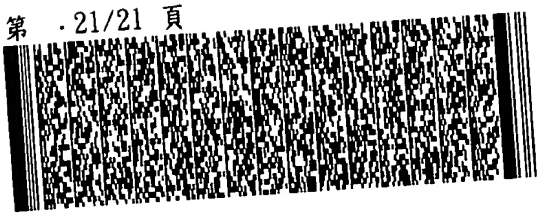
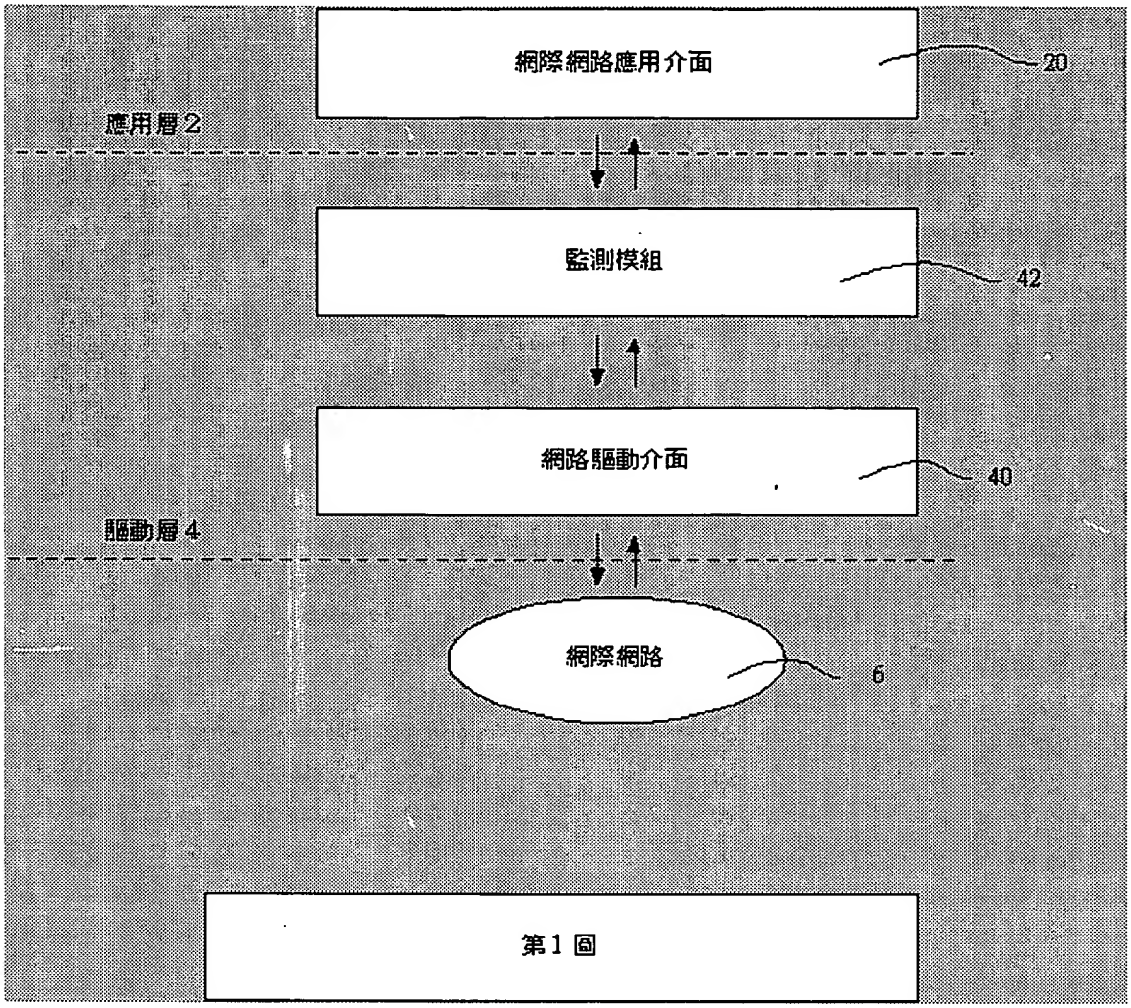
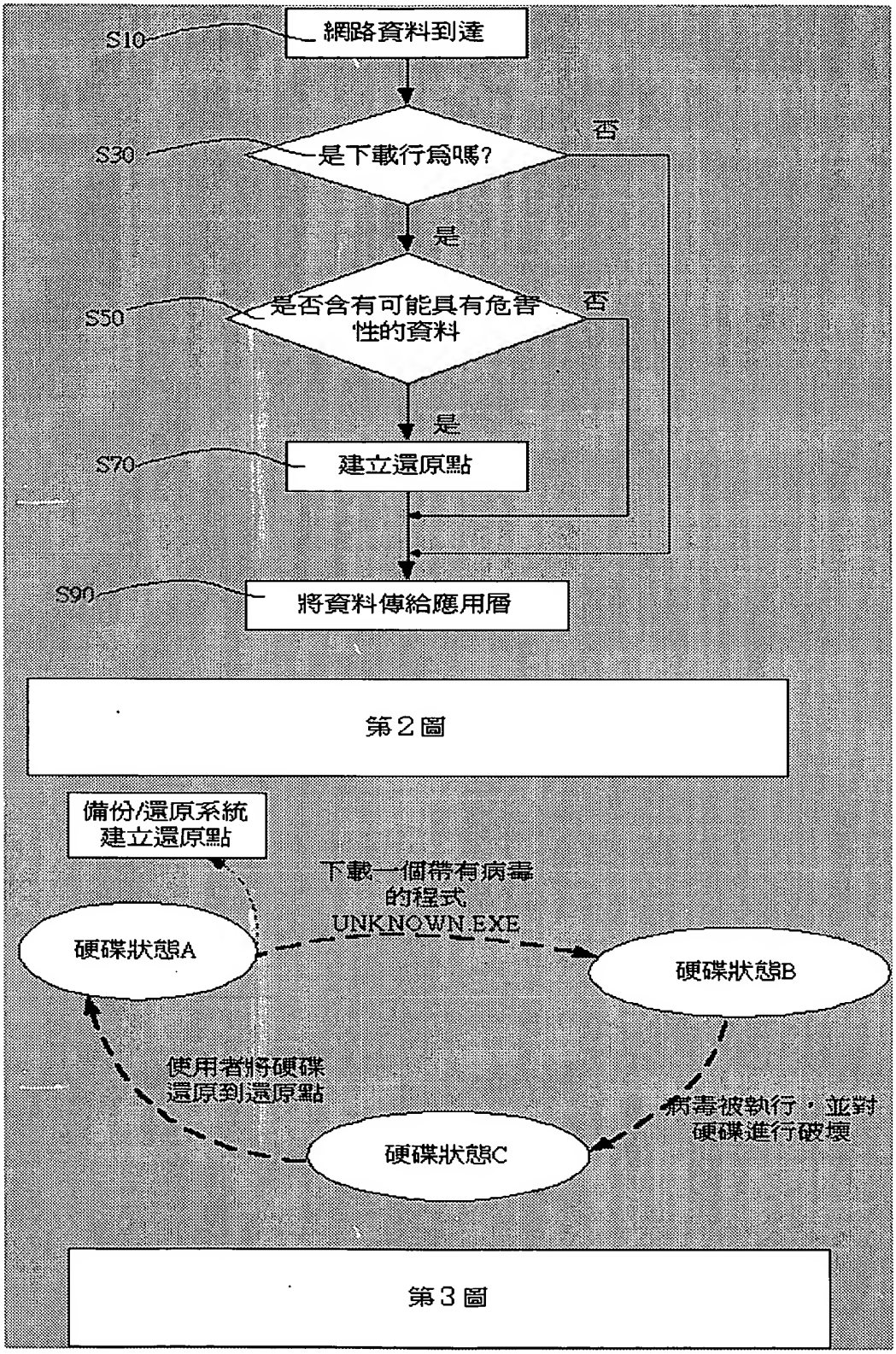


圖　式



第 1 圖

圖　式


S10
網路資料到達
S30
是下載行爲嗎?
否
是
S50
是否含有可能具有危害性的資料
否
是
S70
建立還原點
S90
將資料傳給應用層

第２圖

備份/還原系統
建立還原點
下載一個帶有病毒的程式
UNKNOWN.EXE
硬碟狀態A
硬碟狀態B
使用者將硬碟還原到還原點
病毒被執行，並對硬碟進行破壞
硬碟狀態C

第３圖

圖　式